

Ändern der IP-Adresse der Verwaltungsschnittstelle in FTD, das von FMC verwaltet wird

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Konfigurationen](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie die Management-IP-Adresse für das Firewall Threat Defense-Gerät ändern, das vom Secure Firewall Management Center verwaltet wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defense (FTD)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Secure Firewall Management Center Virtual Running Version 7.2.5(1)
- Cisco Secure Firewall Threat Defense Virtual mit Version 7.2.4

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Konfigurationen

Schritt 1: Navigieren Sie zur FMC-GUI, und wechseln Sie zu Device > Device Management (Gerät > Geräteverwaltung).

Schritt 2: Wählen Sie Device (Gerät) aus, und suchen Sie im Abschnitt Management nach diesem Eintrag.

The screenshot displays the Cisco Firepower Management Center (FMC) configuration interface for a device named 'Frepower'. The 'Device' tab is selected in the top navigation bar. The 'Management' section is highlighted with a red box, showing a toggle switch for management that is currently turned on. Other sections include General, License, System, Inspection Engine, Health, Inventory Details, Applied Policies, and Advanced Settings.

Section	Field	Value	
General	Name	Frepower	
	Transfer Packets	Yes	
	Mode	Routed	
	Compliance Mode	None	
	TLS Crypto Acceleration	Disabled	
	Device Configuration	Import Export Download	
License	Performance Tier	FTDv50 - Tiered (Core 12 / 24 GB)	
	Base	Yes	
	Export-Controlled Features	No	
	Malware	Yes	
	Threat	Yes	
	URL Filtering	Yes	
System	Model	Cisco Firepower Threat Defense for VMware	
	Serial	9A0HJUS0J27	
	Time	2024-04-12 00:57:32	
	Time Zone	UTC (UTC+0:00)	
Inspection Engine	Inspection Engine	Snort 3	
	Revert to Snort 2		
Health	Status	Initial_Health_Policy 2024-04-08 17:12:48	
	Policy	Initial_Health_Policy 2024-04-08 17:12:48	
	Excluded	None	
Inventory Details	CPU Type	CPU Xeon 4100/6100/8100 series 2700 MHz	
	CPU Cores	1 CPU (4 cores)	
	Memory	8192 MB RAM	
	Storage	N/A	
	Chassis URL	N/A	
	Chassis Serial Number	N/A	
	Chassis Module Number	N/A	
	Chassis Module Serial Number	N/A	
	Applied Policies	Access Control Policy	Default
		Prefilter Policy	Default Prefilter Policy
SSL Policy			
DNS Policy		Default DNS Policy	
Identity Policy			
NAT Policy			
Platform Settings Policy			
Advanced Settings	Application Bypass	No	
	Bypass Threshold	3000 ms	
	Object Group Search	Enabled	
	Interface Object Optimization	Disabled	

Schritt 3: Deaktivieren Sie die Verwaltung, indem Sie auf den Schieberegler klicken, und bestätigen Sie die Aktion, indem Sie Ja auswählen.

Frepower
Cisco Firepower Threat Defense for VMware

Device Routing Interfaces Inline Sets DHCP VTEP

General	License	System
Name: Frepower	Performance Tier: FTDv50 - Tiered (Core 12 / 24 GB)	Model: Cisco Firepower Threat Defense for VMware
Transfer Packets: Yes	Base: Yes	Serial: 9A0HJUS0J27
Mode: Routed	Export-Controlled Features: No	Time: 2024-04-12 01:14:15
Compliance Mode: None	Malware: Yes	Time Zone: UTC (UTC+0:00)
TLS Crypto Acceleration: Disabled	Threat: Yes	Version: 7.2.4
	URL Filtering: Yes	Time Zone setting for Time based Rules: UTC (UTC+0:00)
	AnyConnect Apex: No	
	AnyConnect Plus: No	
	AnyConnect VPN O: No	

Device Configuration: [Import](#) [Export](#) [Download](#)

Inspection Engine	Health	Management
Inspection Engine: Snort 3	Status: ●	Host: 192.168.10.42
Return to Snort 2	Policy: 2024-04-08 17:11	Manager Access Interface: Management Interface
	Excluded: None	

Inventory Details

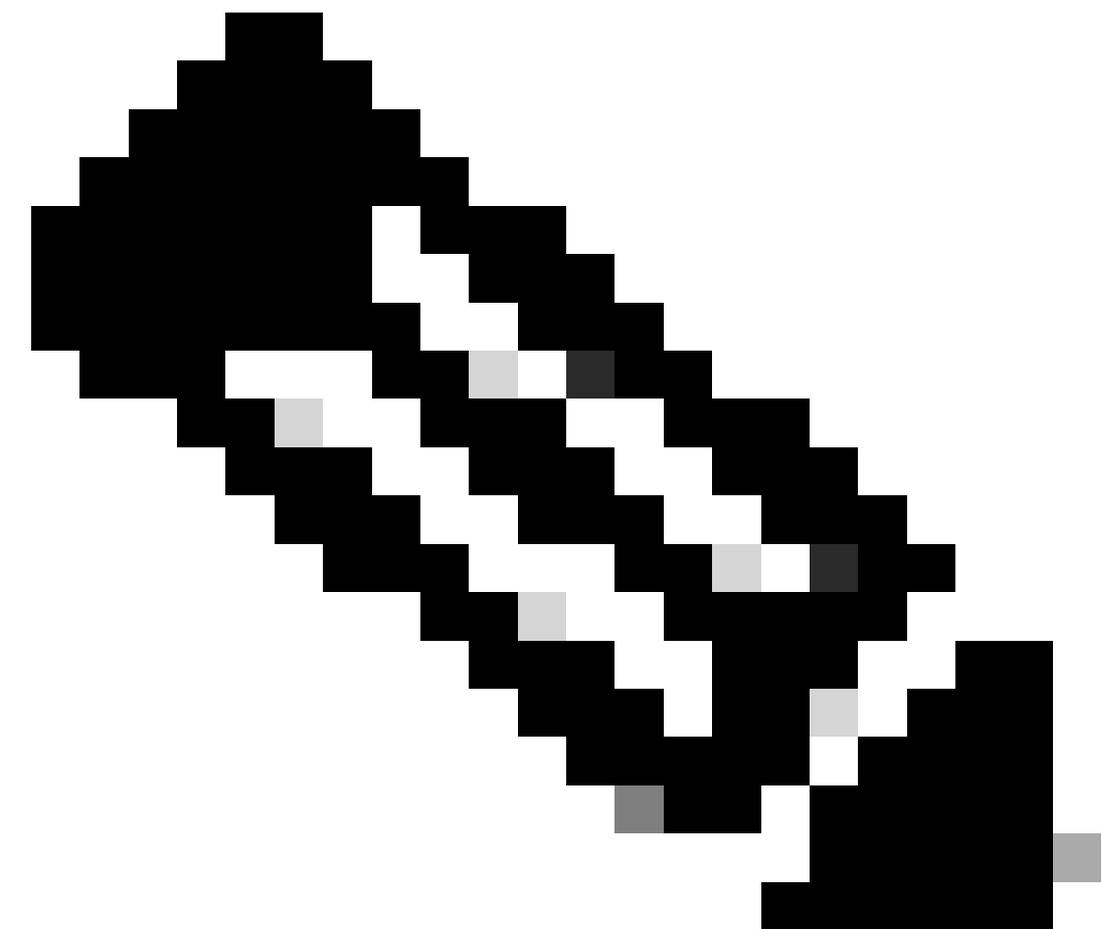
CPU Type: CPU Xeon 4100/6100/8100 series 2700 MHz
CPU Cores: 1 CPU (4 cores)
Memory: 8192 MB RAM
Storage: N/A

Applied Policies	Advanced Settings
Access Control Policy: Default	Application Bypass: No
Prefilter Policy: Default Prefilter Policy	Bypass Threshold: 3000 ms
SSL Policy:	Object Group Search: Enabled
DNS Policy: Default DNS Policy	Interface Object Optimization: Disabled
Identity Policy:	

Disable Management

Managing this device will not be possible if its Management IP is disabled. Do you want to proceed? You can enable it later.

[No](#) [Yes](#)

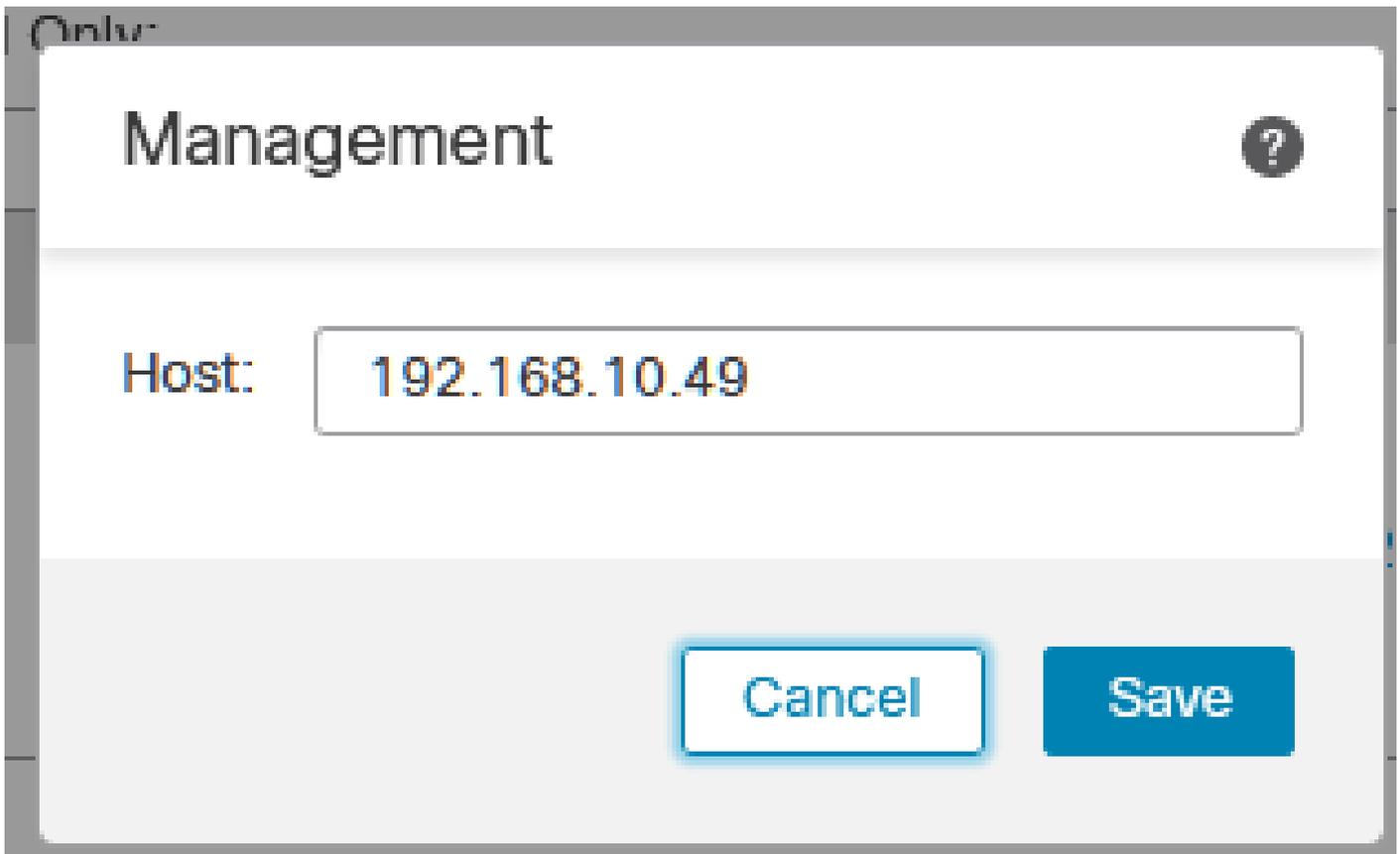


Hinweis: Durch das Ausschalten der Verwaltung wird die Verbindung zwischen dem

Verwaltungszentrum und dem Gerät unterbrochen, das Gerät bleibt jedoch im Verwaltungszentrum.

Schritt 4: Wenn die Verwaltung deaktiviert ist, bearbeiten Sie die Verwaltungsverbindung, indem Sie Bearbeiten auswählen.

Schritt 5: Ändern Sie im Dialogfeld Management die IP-Adresse im Feld für die Remote-Host-Adresse, und wählen Sie dann Speichern aus.



The image shows a dialog box titled "Management" with a question mark icon in the top right corner. Below the title bar, there is a label "Host:" followed by a text input field containing the IP address "192.168.10.49". At the bottom of the dialog, there are two buttons: "Cancel" and "Save".

Schritt 6: Stellen Sie eine Verbindung zur FTD-Konsole her, um die Management-IP-Adresse zu ändern.



Warnung: Wenn Sie die Management-IP-Adresse ändern, kann die SSH-Verbindung zum Gerät unterbrochen werden, wenn die Sitzung über die Management-IP-Adresse hergestellt wird. Es wird daher empfohlen, diese Änderung über den Konsolenzugriff auszuführen, wie von Cisco vorgeschlagen.

Schritt 7. Ändern Sie im Clientmodus die Management-IP-Adresse mit dem folgenden Befehl:

```
> configure network ipv4 manual 192.168.10.49 255.255.0.0 192.168.255.254
```



Hinweis: Diese Konfiguration wird standardmäßig auf die Management-Schnittstelle angewendet.

Schritt 8: Kehren Sie zur FMC-GUI zurück, und aktivieren Sie die Verwaltung durch Umschalten des Schiebereglers auf die Position Ein wieder.

Management 		
Host:		192.168.10.49
Status:		
Manager Access Interface:		Management Interface

Schritt 9. Beachten Sie, dass die Wiederherstellung der Management-Verbindung einige Zeit in

Anspruch nehmen kann. Eine erfolgreiche Wiederherstellung der Verbindung wird in der folgenden Abbildung dargestellt:



Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Sie können die Management-Verbindung über die FTD-CLI überprüfen. Dies wird erreicht, indem im Clientmodus, der diesen Befehl ausführt, eine Verbindung zur CLI hergestellt wird:

```
> sftunnel-status
```

```
SFTUNNEL Start Time: Fri Apr 12 01:27:55 2024
```

```
-----OUTPUT OMITTED-----
```

```
*****
```

```
**RPC STATUS**192.168.10.40*****
```

```
'last_changed' => 'Fri Apr 12 01:09:19 2024',  
'active' => 1,  
'ipv6' => 'IPv6 is not configured for management',  
'uuid_gw' => '',  
'uuid' => '4a6e43f6-f5c7-11ee-97d5-a1dcfaf53393',  
'name' => '192.168.10.40',  
'ip' => '192.168.10.40'
```

```
Check routes:
```

```
No peers to check
```

Fehlerbehebung

In diesem Abschnitt erhalten Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

- Führen Sie den Befehl `show sftunnel status brief` aus, um den Status der Management-Verbindung über die FTD-CLI zu überprüfen. Beobachten Sie die Ausgabe für eine ausgefallene Verbindung, die durch das Fehlen einer Verbindung mit Details für den Peer-Kanal und fehlende Heartbeat-Informationen angezeigt wird.

```
> sftunnel-status-brief
```

```
PEER:192.168.10.40  
Registration: Completed.  
Connection to peer '192.168.10.40' Attempted at Fri Apr 19 21:14:23 2024 UTC  
Last disconnect time : Fri Apr 19 21:14:23 2024 UTC  
Last disconnect reason : Both control and event channel connections with peer went down
```

Eine fehlerfreie Verbindung zwischen den Geräten wird bestätigt, wenn der Befehl `sftunnel-status-brief` in der FTD-CLI einen Ausgang erzeugt, der Peer-Channel umfasst, die mit Informationen und Heartbeat-Daten verbunden sind.

```
> sftunnel-status-brief
```

```
PEER:192.168.10.40  
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '192.168.10.40' via '192.168.10.40'  
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '192.168.10.40' via '192.168.10.40'  
Registration: Completed.  
IPv4 Connection to peer '192.168.10.40' Start Time: Fri Apr 19 21:12:59 2024 UTC  
Heartbeat Send Time: Fri Apr 19 21:13:00 2024 UTC  
Heartbeat Received Time: Fri Apr 19 21:13:23 2024 UTC  
Last disconnect time : Fri Apr 19 21:12:57 2024 UTC  
Last disconnect reason : Process shutdown due to stop request from PM
```

- Um die Netzwerkkonnektivität zu überprüfen, pingen Sie das Management Center von der Management-Schnittstelle aus, und geben Sie `ping system fmc_ip` in die FTD-CLI ein.

Zugehörige Informationen

- [Grundlagen des Gerätemanagements](#)
- [Technischer Support und Downloads von Cisco](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.